Notice of Allowability	Application No.	Applicant(s)	
	10/029,426	SCHMIDT ET AL.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed on 2/15/06 followed up with telephonic communication held on 5/31/06*.

2. ☒ The allowed claim(s) is/are *1,2,4-11,13-18, 21-24 and 32-35, 37-74*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 5/26/06.
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on 2/15/06.

2. The claims 1-2, 7, 21, 32, 46, 51-65, 67 and 70-73 filed on 2/15/06 have been amended.

3. Claims 3, 12, 19-20 and 25-31 and 36 have been canceled.

4. In the previous Office Action the Oath/Declaration has been objected to because the title of the invention was missing. However, under closer investigation it was found that the Oath/Declaration included the application number, name of inventors, and attorney docket number which was on the specification as filed and as a result the objection to the Oath/Declaration has been withdrawn.

5. It seems that the original form 1449 (Information Disclosure Statement (IDS)) was lost. The form is replaced with the attached, considered and signed IDS forms received from applicant by email.

Examiner Amendment

6. An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the Issue Fee.

Authorization for this Examiner's Amendment was given in a telephone interview with Elizabeth J. Reagan (303.357.1644) on 6/08/06.

7. Please replace the previous claims with version of claims below:

--

1. An enterprise network architecture, comprising:

a first network system including a plurality of ~~one or more~~ first network system domains;

a second network system including a plurality of ~~one or more~~ second network system domains, the second network system being autonomous from the first network system such that the first network system domains are administratively independent from the second network system domains; and

a trust link between a first network system root domain and a second network system root domain, the trust link configured to provide transitive resource access between the plurality of ~~one or more~~ first network system domains and the plurality of ~~one or more~~ second network system domains where the transitive resource access includes remote authentication such that an account managed by the second network system ~~can~~ initiates a request for authentication via a first network system domain, and where it is ~~can be~~ determined from the trust link where to communicate the account request and to authenticate the request via the trust link.

2. An enterprise network architecture as recited in claim 1, wherein:

the first network system root domain is configured for communication with the plurality of ~~one or more~~ first network system domains;

the second network system root domain is configured for communication with the plurality of ~~one or more~~ second network system domains; and

the trust link is further configured to provide transitive security associations between the plurality of ~~one or more~~ first network system domains and the plurality of ~~one or more~~ second network system domains.

3. Canceled

4. An enterprise network architecture as recited in claim 1, wherein the transitive resource access includes the remote authentication to access a resource managed in the second network system, such that the account managed by the second network system can initiate the request for authentication to access the resource via the first network system domain.

5. An enterprise network architecture as recited in claim 1, wherein:

the first network system domain includes a first domain controller;

a second network system domain includes a second domain controller; and

the account managed by the second domain controller can initiate the request for remote network authentication via the first domain controller.

6. An enterprise network architecture as recited in claim 1, wherein:

the first network system domain includes a first domain controller;

a second network system domain includes a second domain controller; and

the account managed by the second domain controller can initiate the request for authentication to access a resource managed in the second network system, the request for authentication communicated from the first domain controller to the second network system via the trust link.

7. An enterprise network architecture as recited in claim 1, wherein:

the first network system root domain is configured for communication with the plurality of ~~one or more~~ first network system domains, an individual first network system domain including a first domain controller;

the second network system root domain is configured for communication with the second network system domains, an individual second network system domain including a second domain controller; and

the account managed by the second domain controller can initiate the request for authentication to access a resource managed by the second domain controller, the request for authentication communicated from the first domain controller to the second domain controller via the first network system root domain, the trust link, and the second network system root domain.

8. An enterprise network architecture as recited in claim 1, wherein the trust link is a one-way trust link initiated by an administrator of the first network system, and wherein the account in the second network system can access resources in the first network

system.

9. An enterprise network architecture as recited in claim 1, wherein the trust link is a one-way trust link initiated by an administrator of the first network system, the one-way trust link configured to provide transitive resource access from the second network system domains to the first network system domains.

10. An enterprise network architecture as recited in claim 1, wherein the trust link is a two-way trust link initiated by a first network system administrator and by a second network system administrator, and wherein the transitive resource access is automatically configured when the trust link is established.

11. An enterprise network architecture as recited in claim 1, wherein the first network system is configured to determine from the trust link where to communicate a request for a resource, the request received from the account managed in the first network system and the resource maintained by the second network system.

12. Canceled

13. An enterprise network architecture as recited in claim 1, wherein the first network system is configured to receive a request to logon to the second network system and determine from the trust link where to communicate the request, and wherein the

second network system is configured to authenticate the request.

14. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure configured to maintain namespaces corresponding to trusted network system domain components.

15. An enterprise network architecture as recited in claim 1, wherein the trust link includes a first network system data structure and a second network system data structure, the first network system data structure configured to maintain trusted namespaces corresponding to the second network system, and the second network system data structure configured to maintain trusted namespaces corresponding to the first network system.

16. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure configured to maintain namespaces corresponding to the second network system, and wherein the first network system is configured to:

maintain the data structure; and

automatically designate which of the namespaces are trusted by the first network system.

17. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure maintained by the first network system, the data structure configured to

maintain namespaces corresponding to trusted second network system domain components, and the trusted second network system domain components being designated as trusted by a first network system administrator.

18. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure maintained by the first network system, the data structure configured to maintain trusted namespaces corresponding to the second network system, and wherein the first network system is configured to receive a request to logon to the second network system and determine from the trusted namespaces where to communicate the request.

19. Canceled.

20. Canceled.

21. An enterprise network architecture as recited in claim 1, wherein the first network system is configured to:

receive an account request to logon to the second network system; and

~~determine from the trust link where to communicate the account request; and~~

provide a security identifier to the second network system, the security identifier corresponding to the account.

22. An enterprise network architecture as recited in claim 1, wherein:

the first network system is configured to determine from the trust link where to communicate a service account request to access a resource maintained by the second network system;

the first network system is further configured to provide a security identifier to the second network system, the security identifier corresponding to a user account maintained by the first network system; and

the second network system is configured to determine from the trust link whether to trust the security identifier to authorize the service account request.

23. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure maintained by the first network system, the data structure configured to maintain trusted namespaces corresponding to the second network system, and wherein the first network system is configured to:

determine from the trusted namespaces where to communicate a logon request received from the account managed in the second network system; and

provide a security identifier to the second network system, the security identifier corresponding to the account.

24. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure maintained by the first network system, the data structure configured to maintain trusted namespaces corresponding to the second network system, and wherein:

the first network system is configured to determine from the trusted namespaces where to communicate a service account request to access a resource maintained by the second network system;

the first network system is further configured to provide a security identifier to the second network system, the security identifier corresponding to a user account maintained by the first network system; and

the second network system is configured to determine from the trusted namespaces whether to trust the security identifier to authorize the service account request.

25. Canceled.

26. Canceled.

27. Canceled.

28. Canceled.

29. Canceled.

30. Canceled.

31. Canceled.

32. A network system domain, comprising:

a root domain controller communicatively linked with a plurality of ~~one or more~~ network system domains in a first network system; and

a trusted domain component configured to define a trust link between the root domain controller and a second network system root domain controller, the second network system root domain controller communicatively linked with a plurality of ~~one or more~~ second network system domains that are administratively independent from the first network system domains, and the trust link being configured to provide transitive resource access between the first network system domains and the second network system domains, the trusted domain component being further configured to provide remote network authentication such that an account managed by a second network system domain ~~can~~ initiates a request for authentication via a first network system domain, and where it is ~~can be~~ determined from the trust link where to communicate the account request and to authenticate the request via the trust link.

33. A network system domain as recited in claim 32, wherein the root domain controller is configured to create the trusted domain component when the trust link is initiated.

34. A network system domain as recited in claim 32, wherein the root domain controller is configured to establish the transitive resource access between the first network system domains and the second network system domains when the trust link is initiated.

35. A network system domain as recited in claim 32, wherein the trusted domain component defines a one-way trust link from the root domain controller to the second network system root domain controller.

36. Canceled.

37. A network system domain as recited in claim 32, wherein the trusted domain component is further configured to provide the remote network authentication to access a resource managed by the second network system domain, such that the account managed by the first network system domain can initiate a request to access the resource, the request communicated from the root domain controller to the second network system root domain controller via the trust link.

38. A network system domain as recited in claim 32, wherein the root domain controller is configured to determine from the trusted domain component where to communicate the request for authentication received from the account managed by the second network system domain.

39. A network system domain as recited in claim 32, wherein the trusted domain component is configured to indicate where to communicate the request for authentication received from the account managed by the second network system domain.

40. A network system domain as recited in claim 32, wherein the root domain controller is configured to determine from the trusted domain component where to communicate a request for a resource, the request received from the account managed by the second network system domain and the resource maintained by the second network system domain.

41. A network system domain as recited in claim 32, wherein the root domain controller is configured to receive a request to logon to the second network system domain, and determine from the trusted domain component to communicate the request to the second network system root domain controller via the trust link.

42. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure configured to maintain trusted namespaces corresponding to the second network system.

43. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure configured to maintain namespaces corresponding to

trusted second network system domain components.

44. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure configured to maintain namespaces corresponding to the second network system, and wherein the root domain controller is configured to maintain the data structure and automatically designate which of the namespaces are trusted by the first network system.

45. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure maintained by the root domain controller, the data structure configured to maintain namespaces corresponding to the second network system, and the namespaces being designated as trusted by a network system administrator.

46. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure maintained by the root domain controller, the data structure configured to maintain trusted namespaces corresponding to the plurality of ~~one or more~~ second network system domains, and wherein the root domain controller is configured to receive a request to logon to the second network system and determine from the trusted namespaces where to communicate the request.

47. A network system domain as recited in claim 32, wherein the trusted domain

component is a data structure configured to maintain trusted namespaces corresponding to the second network system, and wherein the root domain controller is configured to determine from the trusted namespaces where to communicate a request for a resource, the request received from an account managed by the root domain controller and the resource maintained by a second network system domain.

48. A network system domain as recited in claim 32, wherein:

the trusted domain component is a data structure configured to maintain trusted namespaces corresponding to the second network system;

the root domain controller is configured to determine from the trusted namespaces where to communicate a request for a resource, the request received from an account managed by the root domain controller and the resource maintained by a second network system domain; and

the second network system is configured to authorize the request for the resource.

49. A network system domain as recited in claim 32, wherein the root domain controller is configured to:

receive an account request to logon to a second network system domain;

determine from the trusted domain component where to communicate the account request; and

provide a security identifier to the second network system domain controller, the security identifier corresponding to the account.

50. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure maintained by the domain controller, the data structure including trusted namespaces corresponding to the second network system, and wherein the root domain controller is configured to:

determine from the trusted namespaces where to communicate a logon request received from an account managed by a second network system; and

provide a security identifier to the second network system domain controller, the security identifier corresponding to the account.

51. A method performed by a first network system domain controller, the ~~performing a~~ method comprising:

establishing a trust link with a second network system domain controller to provide transitive resource access between domains in a first network system and domains in a separate, autonomous second network system;

receiving an authentication request from an account managed by a domain in the second network system; and

determining from the trust link where to communicate the request and ~~to~~ authenticateing the request via the trust link.

52. A The method as recited in claim 51, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

creating a data structure to maintain the network system identifiers; and

designating which of the network system identifiers to trust.

53. A The method as recited in claim 51, wherein establishing the trust link comprises:

receiving namespaces corresponding to the second network system;

creating a data structure to maintain the namespaces; and

designating which of the namespaces to trust.

54. A The method as recited in claim 51, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

creating a data structure to maintain the network system identifiers;

determining whether to trust an individual network system identifier; and

designating in the data structure whether to trust the individual network system identifier.

55. A The method as recited in claim 51, wherein establishing the trust link comprises:

receiving namespaces corresponding to the second network system;

creating a data structure to maintain the namespaces;

determining whether to trust an individual namespace; and

designating in the data structure whether to trust the individual namespace.

56. A The method as recited in claim 51, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

comparing a received network system identifier with existing network system identifiers to determine whether to accept the received network system identifier; and

creating a data structure to maintain accepted network system identifiers.

57. A The method as recited in claim 51, wherein establishing the trust link comprises:

receiving namespaces corresponding to the second network system;

comparing a received namespace with existing namespaces to determine whether to accept the received namespace; and

creating a data structure to maintain accepted namespaces.

58. A The method as recited in claim 51, wherein establishing the trust link comprises receiving network system identifiers corresponding to the second network system and designating which of the network system identifiers to trust, and wherein determining comprises comparing a component of the request with the network system identifiers to determine that the account is managed in the second network system.

59. A The method as recited in claim 51, further comprising providing a security identifier corresponding to the account to the first network system domain controller, the first network system domain controller comparing the security identifier with stored network system identifiers to determine whether the security identifier is valid.

60. A method performed by a first network system domain controller, the ~~performing a~~ method comprising:

establishing a trust link with a second network system domain controller to provide transitive resource access between domains in a first network system and domains in a separate, autonomous second network system;

receiving a resource request from an account managed by the first network system domain controller;

determining from the trust link where to communicate the resource request ~~to communicate the resource request to the second network system~~; and

communicating the resource request to the second network system domain controller via the trust link.

61. A The method as recited in claim 60, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

creating a data structure to maintain the network system identifiers; and

designating which of the network system identifiers to trust.

62. A The method as recited in claim 60, wherein establishing the trust link comprises:

receiving namespaces corresponding to the second network system;

creating a data structure to maintain the namespaces; and

designating which of the namespaces to trust.

63. A The method as recited in claim 60, wherein establishing the trust link comprises receiving network system identifiers corresponding to the second network system and designating which of the network system identifiers to trust, and wherein determining comprises comparing a component of the request with the network system identifiers to determine that the resource is managed in the second network system.

64. A The method as recited in claim 60, further comprising providing a security identifier corresponding to the account to the first network system domain controller, the first network system domain controller comparing the security identifier with stored network system identifiers to determine whether the security identifier is valid.

65. One or more computer-readable media comprising computer-executable instructions that, when executed, direct a first network system domain controller to perform a method comprising:

establishing a trust link with a second network system domain controller to provide transitive resource access between domains in a first network system and domains in a separate, autonomous second network system;

receiving a resource request from an account managed by a domain controller in the second network system;

determining from the trust link to communicate the resource request to the second network system; and

communicating the resource request to the second network system domain controller via the trust link.

66. One or more computer-readable media as recited in claim 65, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

creating a data structure to maintain the network system identifiers; and

designating which of the network system identifiers to trust.

67. One or more computer-readable media comprising computer-executable instructions that, when executed, direct a domain controller in a first network system to perform a method comprising:

requesting network system identifiers corresponding to a second network system to create a trust link between the first network system and the second network system, the second network system being autonomous from the first network system;

the trust link configured to provide transitive resource access between the plurality of first network system domains and the plurality of second network system domains;

determining whether to accept the network system identifiers;

designating accepted network system identifiers as trusted with trust indicators; ~~and~~

creating a data structure to maintain the accepted network system identifiers and corresponding trust indicators;

receiving a resource request from an account managed by the first network system domain controller;

determining from the trust link where to communicate the resource request; and

communicating the resource request via the trust link.

68. One or more computer-readable media as recited in claim 67, wherein determining comprises comparing an individual network system identifier with existing network system identifiers and rejecting the individual network system identifier if it is a duplicate of an existing network system identifier.

69. One or more computer-readable media as recited in claim 67, the method further comprising:

receiving an authentication request to logon to a domain in the second network system;

comparing a component of the authentication request with the network system identifiers; and

communicating the authentication request to the second network system if the component corresponds to a trusted network system identifier.

70. A method of operating a domain controller in a first network system ~~performing a method~~ comprising:

receiving a security identifier from a domain controller in a second network system via a trust link, the security identifier corresponding to an account managed by the second network system;

the trust link configured to provide transitive resource access between the plurality of first network system domains and the plurality of second network system domains;

determining whether the security identifier is valid; ~~and~~

trusting the account corresponding to the security identifier if the security identifier is determined to be valid;

receiving a resource request from an account managed by the first network system domain controller;

determining from the trust link where to communicate the resource request; and

communicating the resource request via the trust link.

71. The A method as recited in claim 70, wherein determining comprises comparing the security identifier with network system identifiers and determining that the security identifier is valid if it matches a component of a network system identifier.

72. The A method as recited in claim 70, wherein determining comprises comparing the security identifier with stored network system identifiers and determining that the security identifier is valid if it matches a component of a network system identifier, the network system identifiers received from the second network system and designated as being trusted when the trust link is initiated.

73. The A method as recited in claim 70, wherein the security identifier corresponds to a security principal managed by the domain controller in the second network system.

74. One or more computer-readable media comprising computer-executable instructions that, when executed, direct a computing system to perform the method of claim 70.

--

Allowable Subject Matter

8. Claims 1-2, 4-11, 13-18, 21-24, 35-35 and 37-73 are allowed.

9. The following is a statement of reasons for the indication of allowable subject matter.

10. The closest prior art Microsoft Windows 2000 discloses a trust link that connects two forests, wherein each forest is a network system that includes a plurality of domains. Although in Windows 2000 the transitive two-way trust is automatically built between a plurality of domains in *a* network system, Windows 2000 does not provide the transitive resource access between a plurality of first and second network system domains wherein the fist and the second system domains are autonomous (administratively independent) from each other (e.g. Gary L. Olsen, "Windows 2000 Active Directory design and deployment, 2000, ISBN: 1578702429, pg. 96) as required by independent claims 1, 32, 51, 60, 65 and 67.

11. Cross certification of Certificate Authorities trust model as illustrated by Menezes (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237) in Fig. 13.9 pg. 574 (c) is another closest prior art that discloses two distinct networks with plurality of domains. Even though the certificate trust model provides transitive authentication that could be used in a transitive access to resources, in the certificate trust model an account resource or authentication request is not resolved by determining from the trust link where to communicate the resource request and communicating the request via the trust link as required by independent claims 1, 32, 51, 60, 65 and 67.

12. The prior art, fails to anticipate or fairly suggest the limitation of applicant's independent claims, in such a manner that a rejection under 35 U.S.C. 102 or 103 would be proper. As a result the claimed invention is considered to be in condition for allowance as being novel and non-obvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on statement of Reasons for Allowance".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached from Monday through Thursday from 9:00 until 5:00, and every other Friday from 9:00 until 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-1600.

6/1/06

JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER